

EXTENDING ELLIPTIC CURVE CHABAUTY TO HIGHER GENUS CURVES

MICHAEL MOURAO

ABSTRACT. We give a generalization of the method of “Elliptic Curve Chabauty” to higher genus curves and their Jacobians. This method can sometimes be used in conjunction with covering techniques and a modified version of the Mordell-Weil sieve to provide a complete solution to the problem of determining the set of rational points of an algebraic curve Y .

CONTENTS

1. Introduction	1
2. Preliminaries	3
3. Chabauty	4
3.1. Unramified Case	5
3.2. Ramified Case	8
3.3. Applying Chabauty	16
4. Mordell-Weil sieve	18
5. Applications to Diophantine Problems	20
5.1. The Equation $y^2 = (x^3 + x^2 - 1)\Phi_{11}(x)$	20
References	24

1. INTRODUCTION

The method of Chabauty and Coleman ([6],[7]) is a very well established and explicit technique used to provide reasonable and sometimes sharp upper bounds for the set of rational points of a curve defined over \mathbb{Q} . To determine the actual set

2010 *Mathematics Subject Classification.* Primary 11G30 ; Secondary 11G20, 11D41, 11D45.

The author is supported by the research grant FCT SFRH/BD/44011/2008. The author would also like to thank Samir Siksek for his valuable comments and guidance.

of rational points, this is usually used in combination with the Mordell-Weil sieve (see for example [3],[4],[5]). One first splits the analytic set of \mathbb{Q}_p -rational points of the curve, where p is a finite rational prime, into a finite disjoint collection of 0, or residue classes as they are often called. Then, Chabauty's argument, made effective using Coleman's integration on these rigid analytic spaces ([8]), often allows one to show that the classes containing known \mathbb{Q} -rational points do not contain any other rational points. The Mordell-Weil sieve is then used to prove that the remaining classes (i.e the ones that appear to have no \mathbb{Q} -rational points), actually have none. The limitation of this method is the fact that it only applies to curves whose Jacobians have Mordell-Weil rank less than or equal to $g - 1$, where g is the genus of the curve.

In a more recent development, Siksek ([10]) showed that when Chabauty's method is generalised to deal with curves defined over a number field of degree $d > 1$ the limitation is usually weakened and the method can be applied to curves whose Jacobians have Mordell-Weil rank less than or equal to $d(g - 1)$.

Often, when one is interested in the set of rational points on a curve Y/\mathbb{Q} , a descent argument leads us to consider the following problem: let C be a curve over a number field K . Let $\psi : C \rightarrow \mathbb{P}^1$ be a morphism defined over K . Determine the set

$$\{P \in C(K) : \psi(P) \in \mathbb{P}^1(\mathbb{Q})\}. \quad (1.1)$$

For example, Bruin ([2]) explains an approach to this when C is a curve of genus 1 using a variant of Chabauty called "Elliptic Curve Chabauty". In the present paper we explain an extension of Bruin's method to the case where the curve C has genus greater than 1. The fact that we are interested not in all K -rational points of C , but in the subset (1.1) allows us to weaken the Chabauty limitation on ranks even further.

Let J be the Jacobian of C . Our method requires knowledge of a subgroup L of $J(K)$ of finite index. Such a subgroup can sometimes, though not always, be computed through a descent calculation (for genus 2 curves see [11]; for cyclic covers of the projective line see [9]).

In Section 2 we start by setting up the notation and presenting how the two techniques described in the latter sections can be combined to determine the set of rational points of an algebraic curve.

In Section 3 the modified version of Chabauty is presented explicitly. There is a slight increase in complexity when dealing with points P_0 on the curve that are ramification points of the morphism ψ , as $\psi - \psi(P_0)$ can no longer be used as a uniformizing parameter in the neighborhoods of these points. This case is thus addressed separately from the case where ψ does not ramify at P_0 . In the end of the section, we apply the results to three examples of curves defined over a quadratic extension of \mathbb{Q} . The outcome of these examples is used in Sections 4 and 5.

Then, in Section 4 we show how the classical Mordell-Weil sieve can also be adapted and refined, in order to work together with the version of Chabauty presented in Section 3.

Finally, in Section 5 we give an example of a genus 6 hyperelliptic curve Y defined over \mathbb{Q} by the equation

$$y^2 = (x^3 + x^2 - 1)\Phi_{11}(x),$$

whose set of \mathbb{Q} -rational points cannot be computed using the classical approach. To apply Bruin's "Elliptic Curve Chabauty", one needs to work over the degree 10 number field $\mathbb{Q}[t]/(\Phi_{11}(t))$, and current tools appear to be incapable of computing generators for the Mordell-Weil groups of the associated elliptic curves. We transfer this problem to a collection of auxiliary genus 2 curves $\{C/K\}$, for an appropriate quadratic number field K . Even at this step the rank limiting inequalities given in [10] are not satisfied, but the inequalities that apply to our case, are. An implementation of our techniques in MAGMA([1]) is then used to successfully prove that

$$Y(\mathbb{Q}) = \{\infty\}.$$

2. PRELIMINARIES

Notation 2.1. Let \mathcal{O}_K be the ring of integers of K and let \mathfrak{p} be a prime of \mathcal{O}_K . If A is any K -algebra and $u \in A$, we will denote by $u^{\mathfrak{p}}$, the image of u under the injection $A \rightarrow A \otimes_K K_{\mathfrak{p}}$, where $K_{\mathfrak{p}}$ is the completion of K at \mathfrak{p} .

Definition 2.2. Let V be a non-singular algebraic variety defined over K and let p be a rational prime, unramified in K such that V has good reduction for every $\mathfrak{p} \mid p$. Denote the residue field at \mathfrak{p} by $k_{\mathfrak{p}}$. We define the map $\text{red}_p : V(K) \rightarrow \prod_{\mathfrak{p} \mid p} V(k_{\mathfrak{p}})$ to be the diagonal product of the usual reduction maps $\text{red}_{\mathfrak{p}} : V(K) \rightarrow V(k_{\mathfrak{p}})$. When V is an abelian variety, these maps are actually homomorphisms of abelian groups.

Definition 2.3. Let C/K be a non-singular algebraic curve. For $\mathcal{P} \in \prod_{\mathfrak{p}|p} C(k_{\mathfrak{p}})$ define

$$\mathcal{B}_p(\mathcal{P}) = \{P \in C(K) : \text{red}_p(P) = \mathcal{P}\}$$

and for $P \in C(K)$ define the p -residue class of P to be

$$B_p(P) := \mathcal{B}_p(\text{red}_p(P)).$$

Fix a morphism $\psi : C \rightarrow \mathbb{P}^1$ defined over K . Let

$$\mathcal{G} := \left\{ \mathcal{P} \in \prod_{\mathfrak{p}|p} C(k_{\mathfrak{p}}) : \overline{\psi^{\mathfrak{p}}}(\mathcal{P}_{\mathfrak{p}}) = \overline{\psi^{\mathfrak{q}}}(\mathcal{P}_{\mathfrak{q}}) \in \mathbb{P}^1(\mathbb{F}_p) \quad \forall \mathfrak{p}, \mathfrak{q} \mid p \right\}.$$

and

$$H := C(K) \cap \psi^{-1}(\mathbb{P}^1(\mathbb{Q})).$$

Consider the following commutative diagram

$$\begin{array}{ccc} H & \xrightarrow{\psi} & \mathbb{P}^1(\mathbb{Q}) \\ \text{red}_p \downarrow & & \downarrow \text{red}_p \\ \prod_{\mathfrak{p}|p} C(k_{\mathfrak{p}}) & \xrightarrow{\prod_{\mathfrak{p}|p} \overline{\psi^{\mathfrak{p}}}} & \prod_{\mathfrak{p}|p} \mathbb{P}^1(\mathbb{F}_p) \end{array}$$

Suppose we have a subset $H' \subseteq H$. In practice H' will be the subset of H found through a computer search. The aim of this paper is to provide methods that often allow one to show that

- (a) for all $P \in H'$ we have that $B_p(P) \cap H = \{P\}$ (by using a modification of “Elliptic Curve Chabauty”) and
 - (b) for all $\mathcal{P} \in \mathcal{G} \setminus \text{red}_p(H')$ we have that $\mathcal{B}_p(\mathcal{P}) \cap H = \emptyset$ (by using a modification of the Mordell-Weil sieve).
- (a) and (b) put together imply that $H' = H$.

3. CHABAUTY

In order to produce the bounds given by Chabauty’s method, we first need to use Coleman’s theory of p -adic integration. Let C/K be an irreducible, non-singular algebraic curve defined over a number field K , p be an odd rational prime such that

for each \mathfrak{p} a prime of \mathcal{O}_K with $\mathfrak{p} \mid p$ and residue field $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$, we have that C has good reduction at \mathfrak{p} . Let J/K be the Jacobian variety of C . Fix a basepoint $Q \in C(K)$ and denote by $\iota : C \rightarrow J$ the Abel-Jacobi map given by

$$\iota(P) = [P - Q].$$

Denote by $K_{\mathfrak{p}}$ the completion of K with respect to \mathfrak{p} and by $\mathcal{O}_{\mathfrak{p}}$ the integers of $K_{\mathfrak{p}}$. Let $\mathcal{C}_{/\mathcal{O}_{\mathfrak{p}}}$ and $\mathcal{J}_{/\mathcal{O}_{\mathfrak{p}}}$ be minimal regular proper models for C and J over $\mathcal{O}_{\mathfrak{p}}$. Denote by $\Omega_{C/K_{\mathfrak{p}}}$ and $\Omega_{J/K_{\mathfrak{p}}}$ the $K_{\mathfrak{p}}$ -spaces of global holomorphic 1-forms on C and J . Coleman ([8]) showed that we have a well defined notion of an integral satisfying:

- (i) $\int_P^{P'} \omega = - \int_{P'}^P \omega$.
- (ii) $\int_P^{P'} \omega + \int_{P'}^{P''} \omega = \int_P^{P''} \omega$.
- (iii) $\int_P^{P'} \omega + \int_P^{P'} \omega' = \int_P^{P'} \omega + \omega'$.
- (iv) $\int_P^{P'} \alpha \omega = \alpha \int_P^{P'} \omega$.
- (v) $\int_P^{P'} \iota^* (\omega_J) = \int_{\iota(P)}^{\iota(P')} \omega_J$.

for $\alpha \in K_{\mathfrak{p}}$, $P, P', P'' \in C(K_{\mathfrak{p}})$, $\omega, \omega' \in \Omega_{C/K_{\mathfrak{p}}}$, $\omega_J \in \Omega_{J/K_{\mathfrak{p}}}$ and ι^* the induced isomorphism from $\Omega_{J/K_{\mathfrak{p}}}$ to $\Omega_{C/K_{\mathfrak{p}}}$.

Furthermore, we have the following bilinear pairing

$$\Omega_{C/K_{\mathfrak{p}}} \times J(K_{\mathfrak{p}}) \rightarrow K_{\mathfrak{p}}, \quad \left(\omega, \left[\sum_i P'_i - \sum_i P_i \right] \right) \mapsto \sum_i \int_{P_i}^{P'_i} \omega \quad (3.1)$$

which is $K_{\mathfrak{p}}$ -linear on the left with kernel equal to 0 and \mathbb{Z} -linear on the right with kernel the torsion part of $J(K_{\mathfrak{p}})$.

3.1. Unramified Case. Let C/K be a non-singular algebraic curve of genus g and $\psi : C/K \rightarrow \mathbb{P}^1$ a morphism to \mathbb{P}^1 which is defined over K . Suppose $P_0 \in H := C(K) \cap \psi^{-1}(\mathbb{P}^1(\mathbb{Q}))$. Suppose further that ψ is unramified at P_0 . If $\psi(P_0) = \infty$ replace ψ by $1/\psi$. Now fix a rational prime p such that:

- (p1): p does not ramify in K , i.e. $p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_m$ with the \mathfrak{p}_i distinct prime ideals.
- (p2): C/K has good reduction at \mathfrak{p}_i for $1 \leq i \leq m$.

(p3): The reduced point $\text{red}_{\mathfrak{p}_i}(P_0)$ is not a ramification point of the reduced map $\overline{\psi^{\mathfrak{p}_i}}$ for $1 \leq i \leq m$.

Fix $\mathfrak{p} \in \{\mathfrak{p}_1, \dots, \mathfrak{p}_m\}$. Let $\mathcal{C}_{/\mathcal{O}_{\mathfrak{p}}}$ be a proper regular minimal model for C over $\mathcal{O}_{\mathfrak{p}}$. Now $\tau := \psi - \psi(P_0) \in K(C)$ is a uniformizer for C/K at P_0 . By **(p1)**, **(p2)** and **(p3)** $\tau^{\mathfrak{p}}$ is a well-behaved uniformizer for the generic fibre \mathcal{C}_0 at P_0 and $\overline{\tau^{\mathfrak{p}}}$ is a uniformizer for the special fibre $\mathcal{C}_{\mathfrak{p}}$ at $\text{red}_{\mathfrak{p}}(P_0)$. Equivalently $\tau^{\mathfrak{p}}$ together with π , a uniformizer of $K_{\mathfrak{p}}$, generate the maximal ideal of the local ring \mathcal{O}_{C, P_0} . Let $P \in B_p(P_0) \cap H$.

Let $\omega_1^{\mathfrak{p}}, \dots, \omega_g^{\mathfrak{p}}$ be a basis for the $\mathcal{O}_{\mathfrak{p}}$ -module $\Omega_{\mathcal{C}_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}}$ of holomorphic 1-forms on $\mathcal{C}_{/\mathcal{O}_{\mathfrak{p}}}$.

Suppose that $L = \langle D_1, \dots, D_r \rangle$ is a finite index subgroup of the Mordell-Weil group $J(K)$ and that $[J(K) : L] = N$. Suppose further that

$$N[P - P_0] = n'_1 D_1 + \dots + n'_r D_r \quad (3.2)$$

in $J(K)$. Set $n_q = n'_q/N \in \mathbb{Q}$ for $1 \leq q \leq r$. Note that

$$t^{\mathfrak{p}} := \tau^{\mathfrak{p}}(P) = \psi^{\mathfrak{p}}(P) - \psi^{\mathfrak{p}}(P_0) = (\psi(P) - \psi(P_0))^{\mathfrak{p}} = \psi(P) - \psi(P_0) \in \mathbb{Q}$$

for every $\mathfrak{p} \mid p$, so

$$t^{\mathfrak{p}_1} = \dots = t^{\mathfrak{p}_m} =: t$$

and since $\text{ord}_{\mathfrak{p}_c}(t^{\mathfrak{p}_c}) \geq 1$ for $1 \leq c \leq m$ we have that $\text{ord}_p(t) \geq 1$. In other words, $t \in p\mathbb{Z}_p$.

We shall need the following standard result.

Lemma 3.1. *Let p be an odd rational prime that does not ramify in K . Let \mathfrak{p} be a prime of \mathcal{O}_K with $\mathfrak{p} \mid p$. Fix a minimal regular model $\mathcal{C}_{/\mathcal{O}_{\mathfrak{p}}}$ for C over $\mathcal{O}_{\mathfrak{p}}$. Let $P_0 \in C(K_{\mathfrak{p}})$ and let $\tau \in K(C)$ be a well-behaved uniformizer at P_0 . Let $\omega \in \Omega_{\mathcal{C}_{/\mathcal{O}_{\mathfrak{p}}}}$, and write*

$$\alpha = \left. \frac{\omega}{d\tau} \right|_{\tau=0}.$$

Then $\alpha \in \mathcal{O}_{\mathfrak{p}}$. Moreover, for all $P \in B_p(P_0)$,

$$\int_{P_0}^P \omega = \alpha \tau(P) + \beta \tau(P)^2 \quad (3.3)$$

for some $\beta \in \mathcal{O}_{\mathfrak{p}}$ (which depends on P).

Proof. For a proof of this see [10] Lemma 3.1 □

Let $\mathfrak{p} \mid p$ and $\omega \in \Omega_{\mathcal{C}/\mathcal{O}_{\mathfrak{p}}}$ be a holomorphic 1-form. We will define the matrix $A_{\mathfrak{p},\omega} \in M_{d_{\mathfrak{p}},r}(\mathbb{Q}_p)$ and the column vector $\mathbf{w}_{\mathfrak{p},\omega} \in \mathbb{Z}_p^{d_{\mathfrak{p}}}$, where $d_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p]$, as follows: Using (3.2) and (3.3) together we get the following equality in $K_{\mathfrak{p}}$

$$\alpha_1 n_1 + \dots + \alpha_r n_r = \alpha t + \beta t^2, \quad (3.4)$$

where $\alpha_q = \int_{D_q} \omega$ for $1 \leq q \leq r$. Fix an integral basis $\theta_1, \dots, \theta_{d_{\mathfrak{p}}}$ for $\mathcal{O}_{\mathfrak{p}}$ over \mathbb{Z}_p . We can write $\alpha_q = a_{1,q}\theta_1 + \dots + a_{d_{\mathfrak{p}},q}\theta_{d_{\mathfrak{p}}}$, $\alpha = a_1\theta_1 + \dots + a_{d_{\mathfrak{p}}}\theta_{d_{\mathfrak{p}}}$ and $\beta = b_1\theta_1 + \dots + b_{d_{\mathfrak{p}}}\theta_{d_{\mathfrak{p}}}$ and equate coefficients to get the following system of equations in \mathbb{Q}_p

$$\begin{aligned} a_{1,1}n_1 + \dots + a_{1,r}n_r &= a_1t + b_1t^2 \\ \vdots &= \vdots \\ a_{d_{\mathfrak{p}},1}n_1 + \dots + a_{d_{\mathfrak{p}},r}n_r &= a_{d_{\mathfrak{p}}}t + b_{d_{\mathfrak{p}}}t^2. \end{aligned}$$

Define $A_{\mathfrak{p},\omega} = (a_{c,q})_{1 \leq c \leq d_{\mathfrak{p}}, 1 \leq q \leq r}$ and $\mathbf{w}_{\mathfrak{p},\omega}$ to be the column vector $(a_1, \dots, a_{d_{\mathfrak{p}}}) \in \mathbb{Z}_p^{d_{\mathfrak{p}}}$.

Now define the matrix $A_{\mathfrak{p}} \in M_{gd_{\mathfrak{p}},r}(\mathbb{Q}_p)$ and the column vector $\mathbf{w}_{\mathfrak{p}} \in \mathbb{Z}_p^{gd_{\mathfrak{p}}}$ as

$$A_{\mathfrak{p}} = \begin{pmatrix} A_{\mathfrak{p},\omega_1^{\mathfrak{p}}} \\ \vdots \\ A_{\mathfrak{p},\omega_g^{\mathfrak{p}}} \end{pmatrix} \quad \text{and} \quad \mathbf{w}_{\mathfrak{p}} = \begin{pmatrix} \mathbf{w}_{\mathfrak{p},\omega_1^{\mathfrak{p}}} \\ \vdots \\ \mathbf{w}_{\mathfrak{p},\omega_g^{\mathfrak{p}}} \end{pmatrix}.$$

Finally define the matrix $A \in M_{dg,r}(\mathbb{Q}_p)$ and the column vector $\mathbf{w} \in \mathbb{Z}_p^{gd}$ as

$$A = \begin{pmatrix} A_{\mathfrak{p}_1} \\ \vdots \\ A_{\mathfrak{p}_m} \end{pmatrix} \quad \text{and} \quad \mathbf{w} = \begin{pmatrix} \mathbf{w}_{\mathfrak{p}_1} \\ \vdots \\ \mathbf{w}_{\mathfrak{p}_m} \end{pmatrix}.$$

We now have

$$A\mathbf{n} = t\mathbf{w} + t^2\mathbf{w}',$$

where $\mathbf{n} = (n_1, \dots, n_r) \in \mathbb{Q}^r$ and $\mathbf{w}' \in \mathbb{Z}_p^{gd}$. Let h be the smallest non-negative integer such that $p^h A$ has entries in \mathbb{Z}_p and U be the unimodular matrix in $M_{gd,gd}(\mathbb{Z}_p)$ such that

$$A' = U(p^h A)$$

is in Hermite Normal Form. Let j be the number of zero rows of A' and denote by $\mathcal{E}_p(P_0)$ the set containing only the column vector in \mathbb{Z}_p^j formed by the last j rows of $U\mathbf{w}$. The reason for defining the set $\mathcal{E}_p(P_0)$ that only contains a single element will become apparent when we discuss how we deal with the case of ψ being ramified at P_0 in 3.2.

Theorem 3.2. *If the unique $E \in \mathcal{E}_p(P_0)$ satisfies $\overline{E} \neq \mathbf{0}$ modulo p , then $B_p(P_0) \cap H = \{P_0\}$.*

Proof. Let $P \in B_p(P_0)$ with $P \neq P_0$ and $\psi(P) \in \mathbb{P}^1(\mathbb{Q})$. Using the fact that $\psi - \psi(P_0)$ is a local isomorphism we see that

$$s = \text{ord}_p(t)$$

is finite. We have that for the unique $E \in \mathcal{E}_p(P_0)$

$$tE + t^2 \mathbf{w}'' = \mathbf{0},$$

where \mathbf{w}'' is the vector formed by the last j rows of $U\mathbf{w}'$. Now divide by p^s and reduce modulo p to get that

$$v\overline{E} \equiv \mathbf{0} \pmod{p}.$$

But this is a contradiction since both v and \overline{E} are non-zero modulo p . \square

3.2. Ramified Case. Suppose we have $P_0 \in H'$ such that ψ ramifies at P_0 . Write $e_\psi(P_0) = e$ for the ramification index of ψ at P_0 . Then $e \geq 2$. Define the modified properties:

(p1)^{split}: $p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_d$, in other words p splits completely in \mathcal{O}_K , and $\gcd(p, e) = 1$.

(p1)^{inert}: $p\mathcal{O}_K = \mathfrak{p}$, in other words p is inert in \mathcal{O}_K .

(p3)^{ram}: $e_{\overline{\psi^p}}(\text{red}_{\mathfrak{p}}(P_0)) = e$ for every prime $\mathfrak{p} \mid p$

If $[K : \mathbb{Q}] = 2$ then choose an odd rational prime p that satisfies either **(p1)^{split}, (p2)** and **(p3)^{ram}** or **(p1)^{inert}, (p2)** and **(p3)^{ram}**, otherwise choose p such that it satisfies **(p1)^{split}, (p2)** and **(p3)^{ram}**.

p splits. Let us first consider the case where K is a number field of degree $d > 1$ over \mathbb{Q} with ring of integers \mathcal{O}_K and that p is an odd rational prime that splits completely over K . Equivalently $p\mathcal{O}_K = \mathfrak{p}_1 \dots \mathfrak{p}_d$ with each \mathfrak{p}_c , $1 \leq c \leq d$, a prime of \mathcal{O}_K of norm equal to p . To simplify the notation let K_c denote the completion of K with respect to \mathfrak{p}_c and \mathcal{O}_c be the ring of integers of K_c . Also let $\mathcal{C}_{/\mathcal{O}_c}$ be a minimal, regular and proper model for C over \mathcal{O}_c .

Lemma 3.3. *Suppose that $P_0 \in H$ has $e_\psi(P_0) = e \geq 2$ and let p be a prime satisfying $(p1)^{\text{split}}, (p2)$ and $(p3)^{\text{ram}}$. Let τ_c be a well-behaved uniformizer of $\mathcal{C}_{/\mathcal{O}_c}$ at P_0 and denote by*

$$v_c T_c^e + \sum_{i=1}^{\infty} \rho_{c,i} T_c^{e+i} \in K_{\mathfrak{p}_c}[[T_c]] = \mathbb{Q}_p[[T_c]]$$

the formal powerseries expansion of $\psi^{\mathfrak{p}_c} - \psi(P_0)$ in terms of τ_c . Suppose there exists $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$. Then for every $c \in \{2, \dots, d\}$, $v_1 T_1^e - v_c T_c^e \in \mathbb{Z}_p[T_1, T_c]$ has a linear factor $T_1 - \hat{\gamma}_c T_c$ satisfying

$$t_1 - \hat{\gamma}_c t_c \equiv 0 \pmod{p^{s(e+1)}},$$

where $t_c := \tau_c(P)$ for $1 \leq c \leq d$ and $s = \text{ord}_p(t_1) = \text{ord}_p(t_c) \geq 1$.

Proof. By substituting P in the powerseries expansion of $\psi^{\mathfrak{p}_c} - \psi(P_0)$ we get the d equations

$$\psi(P)^{\mathfrak{p}_c} - \psi(P_0) = v_c t_c^e + \rho_c t_c^{e+1}$$

where $v_c \in \mathbb{Z}_p^*$, since p satisfies $(p3)^{\text{ram}}$, and $\rho_c \in \mathbb{Z}_p$. Since $\psi(P) \in \mathbb{Q}$ we have that

$$\psi(P)^{\mathfrak{p}_1} = \dots = \psi(P)^{\mathfrak{p}_d} = \psi(P) \in \mathbb{Q}.$$

In particular we have that

$$\text{ord}_p(t_1) = \dots = \text{ord}_p(t_d),$$

since $v_c \in \mathbb{Z}_p^*$ for every $c \in \{1, \dots, d\}$. Let us denote this positive integer by s . We have the following $d-1$ congruences

$$v_1 t_1^e - v_c t_c^e \equiv 0 \pmod{p^{s(e+1)}},$$

for $c \in \{2, \dots, d\}$. By letting $\gamma_c = \frac{t_1}{t_c}$ we have that γ_c is a solution to

$$v_1 X^e - v_c \equiv 0 \pmod{p^{se}}.$$

Since the derivative of this polynomial is equal to eX^{e-1} and e and γ_c are units modulo p we can use Hensel's Lemma to lift γ_c to a solution $\hat{\gamma}_c \in \mathbb{Z}_p^*$. We then have that

$$(X - \hat{\gamma}_c) \mid (v_1 X^e - v_c) \quad \text{and} \quad (T_1 - \hat{\gamma}_c T_c) \mid (v_1 T_1^e - v_c T_c^e).$$

Furthermore we have that

$$\gamma_c \equiv \hat{\gamma}_c \pmod{p^{se}}$$

which implies that

$$t_1 - \hat{\gamma}_c t_c \equiv 0 \pmod{p^{s(e+1)}}.$$

□

Let $P_0, e, p, t_1, \dots, t_d, v_1, \dots, v_d$ be as in the statement of Lemma 3.3 above. Suppose that $(X - \hat{\gamma}_c^{(1)}), \dots, (X - \hat{\gamma}_c^{(l_c)})$ are all the linear factors of $v_1 X^e - v_c$ for $c \in \{2, \dots, d\}$. Define the matrices $E_{(i_2, \dots, i_d)} \in M_{d-1, d}(\mathbb{Z}_p)$ by

$$E_{(i_2, \dots, i_d)} = \begin{pmatrix} 1 & -\hat{\gamma}_2^{(i_2)} & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & \dots & -\hat{\gamma}_d^{(i_d)} \end{pmatrix}$$

for $i_c \in \{1, \dots, l_c\}$.

Let $\{\omega_f^c\}_{1 \leq f \leq g}$ be a basis of $\Omega_{\mathcal{C}/\mathcal{O}_c}$ for $1 \leq c \leq d$ and let $L_0 = \langle D_1, \dots, D_r \rangle$ be a subgroup of $J(K)$ of index $N \in \mathbb{Z}_{>0}$. Now fix a $c \in \{1, \dots, d\}$. Define A_c to be the $g \times r$ matrix with entries in \mathbb{Q}_p defined by $A_c = (a_{f,q})_{1 \leq f \leq g, 1 \leq q \leq r}$ where

$$a_{f,q} = \int_{D_q} \omega_f^c$$

and by \mathbf{w}_c the $g \times d$ matrix with zero entries everywhere apart from the c -th column which will consist of the vector (a_1, \dots, a_g) where a_f is the coefficient of the linear term in the (formal) powerseries expansion of

$$\int_{[P-P_0]} \omega_f^c$$

in terms of τ_c (the uniformizer of $\mathcal{C}/\mathcal{O}_c$ at P_0). Now let A be the $dg \times r$ matrix

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_d \end{pmatrix}$$

with entries in \mathbb{Q}_p and \mathbf{w} be the $gd \times d$ matrix

$$\mathbf{w} = \begin{pmatrix} \mathbf{w}_1 \\ \vdots \\ \mathbf{w}_d \end{pmatrix}$$

with entries in \mathbb{Z}_p . Let h be the smallest non-negative integer such that $p^h A$ has entries in \mathbb{Z}_p and $U \in \mathrm{GL}_{dg}(\mathbb{Z}_p)$ be the unimodular matrix such that

$$A' = U(p^h A)$$

is in Hermite Normal Form. We denote by $E_0 \in M_{j,d}(\mathbb{Z}_p)$ the matrix formed by the last j rows of $U\mathbf{w}$, where j is the number of zero rows of A' . Finally define the set

$$\mathcal{E}_p(P_0) = \begin{cases} \emptyset & \text{if } v_1 X^e - v_c \text{ has no linear} \\ & \text{factors for some } c \in \{2, \dots, d\}, \\ \left\{ \begin{pmatrix} E_0 \\ E_{(i_2, \dots, i_d)} \end{pmatrix} : 1 \leq i_c \leq l_c \right\} & \text{otherwise.} \end{cases}$$

Theorem 3.4. *Suppose $P_0 \in H$ and p is a rational prime satisfying $(p1)^{split}, (p2)$ and $(p3)^{ram}$. If $\text{rank}_{\mathbb{F}_p}(\overline{E}) = d$ for every $E \in \mathcal{E}_p(P_0)$ or if $\mathcal{E}_p(P_0) = \emptyset$, then $B_p(P_0) \cap H = \{P_0\}$.*

Proof. Let $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$. Since $P \neq P_0$ there exist integers n'_1, \dots, n'_r , not all zero, such that

$$N[P - P_0] = n'_1 D_1 + \dots + n'_r D_r$$

in $J(K)$. Let τ_c be a well-behaved uniformizer for $\mathcal{C}_{/\mathcal{O}_c}$ at P_0 , for $c \in \{1, \dots, d\}$. Now

$$n_1 \int_{D_1} \omega_f^c + \dots + n_r \int_{D_r} \omega_f^c = \int_{[P-P_0]} \omega_f^c = \alpha_c^{(f)} t_c + \beta_c^{(f)} t_c^2$$

where $n_q = n'_q/N$ for $q \in \{1, \dots, r\}$. Writing this in terms of matrices we get

$$A\mathbf{n} = \mathbf{w}\mathbf{t} + \mathbf{w}'\mathbf{t}'$$

where \mathbf{t} and \mathbf{t}' are the column vectors (t_1, \dots, t_d) and (t_1^2, \dots, t_d^2) respectively. Multiplying by the unimodular matrix U and looking at the last j rows we see that

$$\mathbf{0} = E_0 \mathbf{t} + \mathbf{w}'' \mathbf{t}'.$$

Dividing by p^s and reducing modulo p we see that

$$\mathbf{0} \equiv \overline{E_0} \mathbf{v} \pmod{p}, \tag{3.5}$$

since $s \geq 1$.

Also we can write $\psi(P) - \psi(P_0)$ as a powerseries in t_c for every c . Since the ramification index of $\psi^{\mathfrak{p}_c}$ at P_0 is e by $(p3)^{ram}$, these powerseries will all start from the e -th term. Using these expansions we get the d equalities

$$\psi(P) - \psi(P_0) = v_c t_c^e + \rho_c t_c^{e+1}.$$

By Lemma 3.3 we know that there exist $i_c \in \{1, \dots, l_c\}$ for each $c \in \{2, \dots, d\}$ such that

$$t_1 - \hat{\gamma}_c^{(i_c)} t_c \equiv 0 \pmod{p^{s(e+1)}},$$

where $s = \text{ord}_p(t_1) = \dots = \text{ord}_p(t_d)$. Since $e > 1$ we get that

$$t_1 - \hat{\gamma}_c^{(i_c)} t_c \equiv 0 \pmod{p^{s+1}}.$$

This can be re-written as

$$\mathbf{0} \equiv \overline{E_{(i_2, \dots, i_d)}} \mathbf{t} \pmod{p^{s+1}}.$$

Dividing by p^s and reducing modulo p we obtain that

$$\mathbf{0} \equiv \overline{E_{(i_1, \dots, i_d)}} \mathbf{v} \pmod{p}. \quad (3.6)$$

Relations (3.5) and (3.6) put together imply that there exists $E \in \mathcal{E}_p(P_0)$ with

$$\mathbf{0} \equiv \overline{E} \mathbf{v} \pmod{p}.$$

But this is a contradiction since $\text{rank}_{\mathbb{F}_p}(\overline{E}) = d$ and $\mathbf{v} \not\equiv 0 \pmod{p}$. \square

p inert. Now if we assume that K is a quadratic extension of \mathbb{Q} the following results show how we may also use an odd rational prime p which is inert in K . This might prove useful in practice, since a split prime satisfying the properties needed to perform Chabauty, might be too big for computational purposes. In the following results we denote by \mathfrak{p} the unique prime above p , which has norm p^2 , by $K_{\mathfrak{p}}$ the completion of K with respect to \mathfrak{p} and by $\mathcal{O}_{\mathfrak{p}}$ the ring of integers of $K_{\mathfrak{p}}$. Let $\mathcal{C}_{/\mathcal{O}_{\mathfrak{p}}}$ be a minimal, regular and proper model for C over $\mathcal{O}_{\mathfrak{p}}$.

Lemma 3.5. *Suppose that $[K : \mathbb{Q}] = 2$, $P_0 \in H$ and p is a rational prime that satisfies $(p1)^{\text{inert}}$, $(p2)$ and $(p3)^{\text{ram}}$. Let τ be a well-behaved uniformizer of $\mathcal{C}_{\mathfrak{p}}$ at P_0 and denote by*

$$vT^e + \sum_{i=1}^{\infty} \rho_i T^{e+i} \in K_{\mathfrak{p}}[[T]]$$

the formal expansion of $\psi^{\mathfrak{p}} - \psi(P_0)$ in terms of τ . Write

$$vT^e = (v_1\theta_1 + v_2\theta_2)(T_1\theta_1 + T_2\theta_2)^e = W_1(T_1, T_2)\theta_1 + W_2(T_1, T_2)\theta_2,$$

where $W_1, W_2 \in \mathbb{Z}_p[T_1, T_2]$ are quadratic forms of degree e . Suppose further that $\text{ord}_p(\Delta) = 0$, where Δ is the discriminant of W_2 . Then if there exists $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$, W_2 has a linear factor $g_1T_1 - g_2T_2$ satisfying

$$g_1t_1 - g_2t_2 \equiv 0 \pmod{p^{s(e+1)}},$$

where t_1, t_2 are defined by $\tau(P) = t_1\theta_1 + t_2\theta_2$ and $1 \leq s = \min(\text{ord}_p(t_1), \text{ord}_p(t_2)) < \infty$.

Proof. By substituting P in the powerseries expansion of $\psi^{\mathfrak{p}} - \psi(P_0)$ we get

$$\begin{aligned} \psi^{\mathfrak{p}} - \psi(P_0) = v\tau(P)^e + \rho\tau(P)^{e+1} &= (W_1(t_1, t_2)\theta_1 + W_2(t_1, t_2)\theta_2) + \\ &\quad (W_3(t_1, t_2)\theta_1 + W_4(t_1, t_2)\theta_2), \end{aligned}$$

where $v \in \mathcal{O}_{\mathfrak{p}}^*, \rho \in \mathcal{O}_{\mathfrak{p}}$ and W_3, W_4 are obtained from $\rho(t_1\theta_1 + t_2\theta_2)^{e+1}$ as W_1 and W_2 were obtained from v in the statement of the lemma. Since $\psi(P) \in \mathbb{Q}$, we have that

$$W_2(t_1, t_2) = -W_4(t_1, t_2).$$

Furthermore since $P \neq P_0$ either $t_1 \neq 0$ or $t_2 \neq 0$, so $s := \min(\text{ord}_p(t_1), \text{ord}_p(t_2))$ is finite. Combining this with the fact that $\text{ord}_{\mathfrak{p}}(\tau(P)) \geq 1$ we can see that s is actually a positive integer. We have that

$$W_2(t_1, t_2) \equiv 0 \pmod{p^{s(e+1)}}.$$

By Hensel's Lemma (since $\text{ord}_p(\Delta) = 0$) we have that there exist $g_1, g_2 \in \mathbb{Z}_p$ such that

$$(g_1T_1 - g_2T_2) \mid W_2(T_1, T_2)$$

and

$$g_1t_1 - g_2t_2 \equiv 0 \pmod{p^{s(e+1)}}.$$

□

Let $K, P_0, e, p, t_1, t_2, W_2$ be as in the statement of Lemma 3.5 above. Suppose that $(g_1^{(1)}T_1 - g_2^{(1)}T_2), \dots, (g_1^{(l)}T_1 - g_2^{(l)}T_2)$ are all the linear factors of $W_2(T_1, T_2)$. Define the l matrices $E_{(i)} \in M_{1,2}(\mathbb{Z}_p)$ by

$$E_{(i)} = \begin{pmatrix} g_1^{(i)} & -g_2^{(i)} \end{pmatrix}$$

for $i \in \{1, \dots, l\}$.

Let $\{\omega_f\}_{1 \leq f \leq g}$ be a basis of $\Omega_{\mathcal{C}/\mathcal{O}_p}$, $\{\theta_1, \theta_2\}$ be an integral basis of \mathcal{O}_p over \mathbb{Z}_p , and $L_0 = \langle D_1, \dots, D_r \rangle$ be a subgroup of $J(K)$ of index $N \in \mathbb{Z}_{>0}$. Define $\{A^{(1)}, \dots, A^{(g)}\} \subseteq M_{2,r}(\mathbb{Q}_p)$ to be the matrices whose entries are defined by

$$A_{1,q}^{(f)}\theta_1 + A_{2,q}^{(f)}\theta_2 = \int_{D_q} \omega_f,$$

and for $f \in \{1, \dots, g\}$ define $\mathbf{w}^{(f)} \in M_{2,2}(\mathbb{Z}_p)$ to be the matrix representing in coordinates $\alpha^{(f)}$, the coefficient of the linear term in the (formal) powerseries expansion of $\int_{[P-P_0]} \omega_f$ in terms of the uniformizer τ of $\mathcal{C}/\mathcal{O}_p$ at P_0 . Now let A be the $2g \times r$ matrix

$$A = \begin{pmatrix} A^{(1)} \\ \vdots \\ A^{(g)} \end{pmatrix}$$

with entries in \mathbb{Q}_p and \mathbf{w} be the $2g \times 2$ matrix

$$\mathbf{w} = \begin{pmatrix} \mathbf{w}^{(1)} \\ \vdots \\ \mathbf{w}^{(g)} \end{pmatrix}$$

with entries in \mathbb{Z}_p . Let h be the smallest integer such that $p^h A$ has entries in \mathbb{Z}_p . Again let $U \in \mathrm{GL}_{dg}(\mathbb{Z}_p)$ be the unimodular matrix such that

$$A' = U(p^h A)$$

is in Hermite Normal Form. We denote by $E_0 \in M_{j,d}(\mathbb{Z}_p)$ the matrix formed by the last j rows of $U\mathbf{w}$, where j is the number of zero rows of A' . Finally define the set

$$\mathcal{E}_p(P_0) = \begin{cases} \emptyset & , \text{ if } W(T_1, T_2) \text{ has no linear factors,} \\ \left\{ \begin{pmatrix} E_0 \\ E_{(i)} \end{pmatrix} : 1 \leq i \leq l \right\} & , \text{ otherwise.} \end{cases}$$

Theorem 3.6. *Suppose $[K : \mathbb{Q}] = 2$, $P_0 \in H$ and p is a rational prime satisfying $(p1)^{\text{inert}}, (p2), (p3)^{\text{ram}}$ and that W_2, Δ are defined as in the statement of Lemma 3.5 with $\mathrm{ord}_p(\Delta) = 0$. Then if $\mathrm{rank}_{\mathbb{F}_p}(\overline{E}) = 2$ for every $E \in \mathcal{E}_p(P_0)$ or if $\mathcal{E}_p(P_0) = \emptyset$, we have that $B_p(P_0) \cap H = \{P_0\}$.*

Proof. Let $P \in (B_p(P_0) \cap H) \setminus \{P_0\}$. Since $P \neq P_0$ there exist integers n'_1, \dots, n'_r , not all zero, such that

$$N[P - P_0] = n'_1 D_1 + \dots + n'_r D_r$$

in $J(K)$. Let τ be a well-behaved uniformizer for $\mathcal{C}/\mathcal{O}_{\mathfrak{p}}$ at P_0 . Now

$$n_1 \int_{D_1} \omega_f + \dots + n_r \int_{D_r} \omega_f = \int_{[P-P_0]} \omega_f = \alpha^{(f)} \tau(P) + \beta^{(f)} \tau(P)^2$$

where $n_q = n'_q/N$ for $q \in \{1, \dots, r\}$. Writing this in terms of matrices we get

$$A\mathbf{n} = \mathbf{w}\mathbf{t} + \mathbf{w}'\mathbf{t}'$$

where \mathbf{t} and \mathbf{t}' are the column vectors $\mathbf{t} = (t_1, t_2)$ and $\mathbf{t}' = (t'_1, t'_2)$ with t'_1, t'_2 defined by $\tau(P)^2 = t'_1\theta_1 + t'_2\theta_2$. Multiplying by the unimodular matrix U and looking at the last j rows we see that

$$\mathbf{0} = E_0\mathbf{t} + \mathbf{w}''\mathbf{t}'.$$

Dividing by p^s and reducing modulo p we see that

$$\mathbf{0} \equiv \overline{E_0}\mathbf{v} \pmod{p}, \quad (3.7)$$

since $s \geq 1$.

Also we can write $\psi(P) - \psi(P_0)$ as a powerseries in $\tau(P)$. Since the ramification index of $\psi^{\mathfrak{p}}$ at P_0 is e by $(\mathfrak{p}^3)^{\text{ram}}$, this powerseries will start from the e -th term. By Lemma 3.5 we know that there exists $i \in \{1, \dots, l\}$ such that

$$g_1^{(i)}t_1 - g_2^{(i)}t_2 \equiv 0 \pmod{p^{s(e+1)}},$$

where $s = \min(\text{ord}_p(t_1), \text{ord}_p(t_2))$. Since $e > 1$ we get that

$$g_1^{(i)}t_1 - g_2^{(i)}t_2 \equiv 0 \pmod{p^{s+1}}.$$

This can be re-written as

$$\mathbf{0} \equiv \overline{E_{(i)}}\mathbf{t} \pmod{p^{s+1}}.$$

Dividing by p^s and reducing modulo p we obtain that

$$\mathbf{0} \equiv \overline{E_{(i)}}\mathbf{v} \pmod{p}. \quad (3.8)$$

Relations (3.7) and (3.8) put together imply that there exists $E \in \mathcal{E}_p(P_0)$ with

$$\mathbf{0} \equiv \overline{E}\mathbf{v} \pmod{p}.$$

But this is a contradiction since $\text{rank}_{\mathbb{F}_p}(\overline{E}) = 2$ and $\mathbf{v} \not\equiv 0 \pmod{p}$. \square

3.3. Applying Chabauty.

Example 3.7. Let K be the number field defined by $\mathbb{Q}[x]/(x^2 - x + 3)$, and denote by θ the corresponding image of x in the quotient. Consider the three hyperelliptic curves C_1 , C_2 and C_3 defined over K by the equations

$$C_{1/K} : y^2 = x^5 + \theta x^4 - x^3 + x^2 + (\theta - 1)x - 1 \quad (3.9)$$

$$C_{2/K} : y^2 = -x^5 - \theta x^4 + x^3 - x^2 - (\theta - 1)x + 1 \quad (3.10)$$

$$C_{3/K} : y^2 = (-\theta + 5)x^5 + (4\theta + 3)x^4 + (\theta - 5)x^3 + (-\theta + 5)x^2 + (5\theta - 2)x + \theta - 5 \quad (3.11)$$

and the “ x -coordinate” maps ψ_1, ψ_2, ψ_3 from the projective models of these curves to the projective line

$$\psi_i : C_i \rightarrow \mathbb{P}^1, \quad \psi_i(X, Y, Z) = (X, Z).$$

Denote $C_i(K) \cap \psi_i^{-1}(\mathbb{P}^1(\mathbb{Q}))$ by H_i for $1 \leq i \leq 3$. Let

$$\begin{aligned} H'_1 &:= \{(-1, -1, 1), (-1, 1, 1), (1, 0, 0)\} \subseteq H_1 \\ H'_2 &:= \{(0, 1, 1), (0, -1, 1), (1, 0, 0)\} \subseteq H_2 \\ H'_3 &:= \{(1, 0, 0)\} \subseteq H_3. \end{aligned} \quad (3.12)$$

After searching for K -rational points on C_1 , C_2 and C_3 it appears that actually $H'_1 = H_1$, $H'_2 = H_2$ and $H'_3 = H_3$. The first step towards proving this is using Theorems 3.2, 3.4 and 3.6 together with the relevant information (computed using MAGMA [1]) presented in the following tables:

In TABLE 1 we observe that the rank of the Mordell-Weil group of the Jacobian variety of C_1 is equal to $3 > d(g - 1) = 2$, making it impossible to use the classical method of Chabauty which requires that $r \leq d(g - 1)$. See for example [10]. Our method is applicable in cases where the rank r of $J(K)$ satisfies

$$r \leq dg - 1.$$

In TABLE 2 we give the matrix A with entries in \mathbb{Q}_p and a corresponding unimodular matrix U with entries in \mathbb{Z}_p , such that UA is a matrix in Hermite Normal Form.

Remark 3.8. Since, in practice, we are always working with finite precision, the matrix U presented in TABLE 2 is not unique. This does not however affect the ranks of the matrices \overline{E} for $E \in \mathcal{E}_p(P_0)$.

C	$\text{rank}_{\mathbb{F}_2}(\text{Sel}^{(2)}(J_C/K))$	lin. ind. non-torsion divisors (In Mumford Representation)	$\text{rank}(J_C(K))$
C_1	3	$(x^2 - x + 1, -x + 1)$ $(x^2 + (\theta - 1)x - 1, (\theta - 1)x - 1)$ $(x^2 + (-\theta - 1)x - \theta + 2, (3\theta - 1)x + \theta - 4)$	3
C_2	1	$(x^2 - x - \theta, (\theta - 2)x - 2)$	1
C_3	1	$(x^2 + (2\theta - 1)x + \theta - 3, (-4\theta - 3)x - 5\theta + 2)$	1

TABLE 1. The Mordell-Weil data for C_1 , C_2 and C_3 .

	p	A	U
C_1	89	$\begin{pmatrix} 70 & 82 & 51 \\ 70 & 61 & 86 \\ 55 & 3 & 58 \\ 29 & 38 & 28 \end{pmatrix} \times 89 + O(89^2)$	$\begin{pmatrix} -6 & 1 & -13 & 3 \\ -5 & -1 & 5 & 5 \\ -42 & 0 & 14 & 38 \\ 6 & 2 & -6 & -11 \end{pmatrix} + O(89)$
C_2	23	$\begin{pmatrix} -6 \\ -11 \\ -11 \\ -11 \end{pmatrix} \times 23 + O(23^2)$	$\begin{pmatrix} -2 & 0 & 1 & 0 \\ 1 & 0 & 11 & 1 \\ -11 & 0 & 6 & 0 \\ 0 & 1 & -1 & 0 \end{pmatrix} + O(23)$
C_3	71	$\begin{pmatrix} 58 \\ 60 \\ 47 \\ 48 \end{pmatrix} \times 71 + O(71^2)$	$\begin{pmatrix} 0 & 0 & -1 & 1 \\ 1 & 0 & -13 & 13 \\ 0 & 1 & -11 & 11 \\ 0 & 0 & 23 & -24 \end{pmatrix} + O(71)$

TABLE 2. The period matrices for C_1 , C_2 and C_3 .

P_0	τ	\mathbf{w}	$\{E_{j_2}\}$	$\mathcal{E}_p(P_0)$
$(1, 1, -1)$ unramified	$x + 1$	$\begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} + O(89)$	N/A	$\begin{pmatrix} 9 \end{pmatrix} + O(89)$
$(1, -1, -1)$ unramified	$x + 1$	$\begin{pmatrix} -1 \\ 1 \\ -1 \\ 1 \end{pmatrix} + O(89)$	N/A	$\begin{pmatrix} -9 \end{pmatrix} + O(89)$
$(1, 0, 0)$ ramified	$\frac{(\theta-1)x^2}{2y}$	$\begin{pmatrix} 0 & 0 \\ 41 & 0 \\ 0 & 0 \\ 0 & 79 \end{pmatrix} + O(89)$	$\begin{pmatrix} 1 & 41 \\ 1 & -41 \end{pmatrix} + O(89),$	$\begin{pmatrix} 82 & 21 \\ 1 & 41 \end{pmatrix} + O(89),$ $\begin{pmatrix} 82 & 21 \\ 1 & -41 \end{pmatrix} + O(89)$

TABLE 3. Chabauty data for C_1

Using Theorems 3.2, 3.4 and the data in TABLES 3, 4 and 5 we deduce the following:

- (a) $B_{89}(P_0) \cap H_1 = \{P_0\}$ for every $P_0 \in H'_1$
- (b) $B_{23}(P_0) \cap H_2 = \{P_0\}$ for every $P_0 \in H'_2$
- (c) $B_{71}(P_0) \cap H_3 = \{P_0\}$ for every $P_0 \in H'_3$

P_0	τ	\mathbf{w}	$\{E_{j_2}\}$	$\mathcal{E}_p(P_0)$
$(0, -1, 1)$ unramified	x	$\begin{pmatrix} -1 \\ 0 \\ -1 \\ 0 \end{pmatrix} + O(23)$	N/A	$\begin{pmatrix} 11 \\ 5 \\ 1 \end{pmatrix} + O(23)$
$(0, 1, 1)$ unramified	x	$\begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} + O(23)$	N/A	$\begin{pmatrix} -11 \\ -5 \\ -1 \end{pmatrix} + O(23)$
$(1, 0, 0)$ ramified	$-\frac{\theta+2}{6} \frac{x^2}{y}$	$\begin{pmatrix} 0 & 0 \\ 17 & 0 \\ 0 & 0 \\ 0 & 5 \end{pmatrix} + O(23)$	$\begin{pmatrix} 1 & 3 \\ 1 & -3 \end{pmatrix} + O(23),$ $\begin{pmatrix} 1 & 3 \\ 1 & -3 \end{pmatrix} + O(23)$	$\begin{pmatrix} 0 & 5 \\ 0 & 0 \\ -6 & 0 \\ 1 & 3 \end{pmatrix} + O(23),$ $\begin{pmatrix} 0 & 5 \\ 0 & 0 \\ -6 & 0 \\ 1 & -3 \end{pmatrix} + O(23)$

TABLE 4. Chabauty data for C_2

P_0	τ	\mathbf{w}	$\{E_{j_2}\}$	$\mathcal{E}_p(P_0)$
$(1, 0, 0)$ ramified	$\frac{2(5-\theta)x^2}{y}$	$\begin{pmatrix} 0 & 0 \\ 56 & 0 \\ 0 & 0 \\ 0 & 64 \end{pmatrix} + O(71)$	\emptyset	\emptyset

TABLE 5. Chabauty data for C_3

4. MORDELL-WEIL SIEVE

$$\begin{array}{ccccc}
H & \subseteq & C(K) & \xrightarrow{\iota} & J(K) \\
\downarrow \text{red}_{p_i} & & \downarrow \text{red}_{p_i} & & \downarrow \text{red}_{p_i} \\
\mathcal{G}_i \subseteq \prod_{\mathfrak{p}|p_i} C(k_{\mathfrak{p}}) & \xrightarrow{\iota} & \prod_{\mathfrak{p}|p_i} J(k_{\mathfrak{p}}) & &
\end{array} \tag{4.1}$$

Theorem 4.1. *Let $L = \langle D_1, \dots, D_r \rangle < J(K)$ be a subgroup of the Mordell-Weil group of finite index equal to N and p_0, p_1, \dots, p_b be rational primes satisfying*

- (i) p_i does not ramify in \mathcal{O}_K for $0 \leq i \leq b$.
- (ii) C/K has good reduction for every prime $\mathfrak{p} \mid p_i$, for $0 \leq i \leq b$.
- (iii) $\# \prod_{\mathfrak{p}|p_i} J(k_{\mathfrak{p}})$ is coprime with N for $0 \leq i \leq b$.

Let

$$\mathcal{G}_i = \left\{ \mathcal{P} \in \prod_{\mathfrak{p} | p_i} C(k_{\mathfrak{p}}) : \overline{\psi}_{\mathfrak{p}}(\mathcal{P}_{\mathfrak{p}}) = \psi_{\mathfrak{q}}(\mathcal{P}_{\mathfrak{q}}) \in \mathbb{P}^1(\mathbb{F}_{p_i}) \quad \forall \mathfrak{p}, \mathfrak{q} \mid p_i \right\}.$$

Let $L_0 := L \cap \text{Kernel}(\text{red}_{p_0})$ and define inductively $L_i := L_{i-1} \cap \text{Kernel}(\text{red}_{p_i})$ for $1 \leq i \leq b$. Then for every $\mathcal{P} \in \mathcal{G}_0$ define $W_{0,\mathcal{P}} = \{l \in L/L_0 : \text{red}_{p_0}(w) = \iota(\mathcal{P})\}$ and then inductively $W_{i,\mathcal{P}} := \{w + l : w \in W_{i-1,\mathcal{P}}, l \in L_{i-1}/L_i, \text{red}_{p_i}(w + l) \in \iota(\mathcal{G}_i)\}$ for $1 \leq i \leq b$. Then if $W_{b,\mathcal{P}} = \emptyset$ we have that $\mathcal{B}_{p_0}(\mathcal{P}) \cap H = \emptyset$.

Proof. Suppose there exists some point P in $\mathcal{B}_{p_0}(\mathcal{P}) \cap H$. Then $N\iota(P) = n_1 D_1 + \dots + n_r D_r$ for some $n_1, \dots, n_r \in \mathbb{Z}$. Since condition (iii) holds for p_0 we have that $\text{red}_{p_0}(\iota(P)) \in \text{red}_{p_0}(L)$ and also $\text{red}_{p_0}(\iota(P)) = \iota(\mathcal{P})$ by commutativity of diagram (4.1), in other words we can find $w_{0,P} \in L/L_0$ such that $\text{red}_{p_0}(w_{0,P}) = \text{red}_{p_0}(\iota(P))$. In particular $w_{0,P} \in W_{0,\mathcal{P}}$. Now suppose that for $i = 0, \dots, i-1$ we have $w_{i-1,P} \in W_{i-1,\mathcal{P}}$ such that $\text{red}_{p_{i-1}}(w_{i-1,P}) = \text{red}_{p_{i-1}}(\iota(P))$. We now have

$$\iota(P) - w_{i-1,P} \in \bigcap_{j=0}^{i-1} \text{Kernel}(\text{red}_{p_j}).$$

If we multiply by the index N we have

$$N(\iota(P) - w_{i-1,P}) \in L \cap \left(\bigcap_{j=0}^{i-1} \text{Kernel}(\text{red}_{p_j}) \right) = L_{i-1}$$

and if we reduce both sides modulo p_i we get

$$N \text{red}_{p_i}(\iota(P) - w_{i-1,P}) \in \text{red}_{p_i}(L_{i-1}).$$

But since N is coprime with $\#\text{red}_{p_i}(L_{i-1})$ by (iii) this implies that

$$\text{red}_{p_i}(\iota(P) - w_{i-1,P}) \in \text{red}_{p_i}(L_{i-1}).$$

So there exists $l \in L_{i-1}/L_i$ such that $\text{red}_{p_i}(l) = \text{red}_{p_i}(\iota(P) - w_{i-1,P})$. But we can now define an element of $W_{i,\mathcal{P}}$ by

$$w_{i,P} := w_{i-1,P} + l \in W_{i,\mathcal{P}}.$$

In particular $W_{b,\mathcal{P}}$ is non-empty. □

Example 4.2. Let C_1, C_2 and C_3 be the curves defined in Section 3 (3.9), (3.10) and (3.11). Then

- (a) $\mathcal{B}_{89}(\mathcal{P}) \cap H_1 = \emptyset$ for every $\mathcal{P} \in \prod_{p|89} C_1(k_p) \setminus \text{red}_{89}(H'_1)$. This was shown after taking $\{p_0, p_1, p_2, p_3 = p_b\} = \{89, 673, 859, 131\}$ and using Theorem 4.1 after checking that conditions (i), (ii) and (iii) were satisfied for each of these primes.
- (b) $\mathcal{B}_{23}(\mathcal{P}) \cap H_2 = \emptyset$ for every $\mathcal{P} \in \prod_{p|23} C_2(k_p) \setminus \text{red}_{23}(H'_2)$. The primes used here were $\{23, 43\}$.
- (c) $\mathcal{B}_{71}(\mathcal{P}) \cap H_3 = \emptyset$ for every $\mathcal{P} \in \prod_{p|71} C_3(k_p) \setminus \text{red}_{71}(H'_3)$. The primes used were $\{71, 131\}$.

Lemma 4.3. *Let C_1, C_2 and C_3 be the curves defined in (3.9), (3.10) and (3.11) respectively and let ψ_i for $1 \leq i \leq 3$ be the corresponding “ x -coordinate” maps from the curves to the projective line. We have that $H_i = C_i(K) \cap \psi_i^{-1}(\mathbb{P}^1(\mathbb{Q})) = H'_i$ for $1 \leq i \leq 3$, where the H'_i are as in (3.12).*

Proof. Just note that the corresponding parts of Examples 3.7 and 4.2 together give the required result. \square

5. APPLICATIONS TO DIOPHANTINE PROBLEMS

In this section we consider an example of a curve Y defined over \mathbb{Q} whose set of rational points is computed using the methods presented in the previous sections. This illustrates how all of the existing methods ([2],[6],[7],[10]) may fail due to theoretical or computational restrictions, while the methods in this paper remain applicable. The usefulness of this technique should be more apparent when used on curves that are not hyperelliptic, for example more general cyclic covers of the projective line. These might have Jacobians of Mordell-Weil rank large enough to pose a theoretical obstruction to the use of classical Chabauty or its refinement in [10] and also fail to be related to collections of curves of genus 1, where “Elliptic Curve Chabauty” might be applicable.

5.1. The Equation $y^2 = (x^3 + x^2 - 1)\Phi_{11}(x)$. Let Y be the genus 6 hyperelliptic curve defined by the equation

$$\begin{aligned} y^2 &= (x^3 + x^2 - 1)\Phi_{11}(x) \\ &= x^{13} + 2x^{12} + 2x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 - x - 1. \end{aligned}$$

We prove that

$$Y(\mathbb{Q}) = \{\infty\},$$

using the techniques developed in the previous sections.

We start by noticing that over $K = \mathbb{Q}[x]/(x^2 - x + 3) = \mathbb{Q}(\theta)$,

$$(x^3 + x^2 - 1)\Phi_{11}(x) = (x^3 + x^2 - 1)f(x)g(x)$$

where

$$\begin{aligned} f(x) &= x^5 + \theta x^4 - x^3 + x^2 + (\theta - 1)x - 1 \\ g(x) &= x^5 + (-\theta + 1)x^4 - x^3 + x^2 - \theta x - 1. \end{aligned}$$

Consider the four fibred products of curves defined over K by

$$\begin{aligned} D_1 : & \begin{cases} y_1^2 = x^3 + x^2 - 1 \\ y_2^2 = f(x) \\ y_3^2 = g(x) \end{cases} \\ D_2 : & \begin{cases} y_1^2 = x^3 + x^2 - 1 \\ y_2^2 = -f(x) \\ y_3^2 = -g(x) \end{cases} \\ D_3 : & \begin{cases} y_1^2 = 23(x^3 + x^2 - 1) \\ y_2^2 = (5 - \theta)f(x) \\ y_3^2 = (\theta + 4)g(x) \end{cases} \\ D_4 : & \begin{cases} y_1^2 = 23(x^3 + x^2 - 1) \\ y_2^2 = -(5 - \theta)f(x) \\ y_3^2 = -(\theta + 4)g(x) \end{cases} \end{aligned}$$

and the corresponding covering maps

$$\delta_i : D_i \rightarrow Y, \quad \delta_i(x, y_1, y_2, y_3) = \begin{cases} (x, y_1 y_2 y_3) & \text{for } i = 1, 2 \\ (x, \frac{1}{23} y_1 y_2 y_3) & \text{for } i = 3, 4. \end{cases}$$

For each of these we have another covering map

$$\gamma_i : D_i \rightarrow C_i, \quad \gamma_i(x, y_1, y_2, y_3) = (x, y_2),$$

where C_1 , C_2 and C_3 are the genus 2 hyperelliptic curves defined in Section 3 (3.9), (3.10) and (3.11) and C_4 is the genus 2 hyperelliptic curve defined over K by

$$y^2 = -(5 - \theta)f(x).$$

Lemma 5.1. *Let $H_i := C_i(K) \cap \psi_i^{-1}(\mathbb{P}^1(\mathbb{Q}))$ for $1 \leq i \leq 4$. We have that*

$$Y(\mathbb{Q}) = \bigcup_{i=1}^4 \delta_i(\gamma_i^{-1}(H_i)).$$

Proof. Define the map μ

$$\mu : Y(\mathbb{Q}) \rightarrow (\mathbb{Q}^*/\mathbb{Q}^{*2}) \times (K^*/K^{*2})$$

$$\mu(x, y) = \begin{cases} ((x^3 + x^2 - 1)\mathbb{Q}^{*2}, f(x)K^{*2}) & , \text{ if } (x, y) \neq \infty \\ ((1)\mathbb{Q}^{*2}, (1)K^{*2}) & , \text{ if } (x, y) = \infty \end{cases}$$

The image of this map is contained in

$$\text{Kernel}(\overline{N}) \cap (\mathbb{Q}(2, S_1) \times K(2, S_2)),$$

where $S_1 = \text{Supp}(\text{Resultant}(x^3 + x^2 - 1, f(x)g(x))) = \{23\}$, $S_2 = \text{Supp}(\text{Resultant}(f(x), (x^3 + x^2 - 1)g(x))) = \{\mathfrak{p}\}$, with \mathfrak{p} one of the primes of \mathcal{O}_K above 23, and

$$\overline{N} : (\mathbb{Q}^*/\mathbb{Q}^{*2}) \times (K^*/K^{*2}) \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$$

the reduction of the product of norm maps

$$N : \mathbb{Q} \times K \rightarrow \mathbb{Q},$$

$$N(h_1, h_2) = h_1 N_{K/\mathbb{Q}}(h_2).$$

Also for each element (α_1, α_2) in the image of μ we can associate a cover $\delta_{(\alpha_1, \alpha_2)} : D_{(\alpha_1, \alpha_2)} \rightarrow Y$ defined by

$$D_{(\alpha_1, \alpha_2)} : \begin{cases} y_1^2 = \alpha_1(x^3 + x^2 - 1) \\ y_2^2 = \alpha_2 f(x) \\ y_3^2 = \sigma(\alpha_2)g(x) \end{cases} \quad \text{and}$$

$$\delta_{(\alpha_1, \alpha_2)}(x, y_1, y_2, y_3) = (x, \nu y_1 y_2 y_3),$$

where ν is a rational number satisfying $\nu^2 \alpha_1 N_{K/\mathbb{Q}}(\alpha_2) = 1$. We now have

$$Y(\mathbb{Q}) = \bigcup_{(\alpha_1, \alpha_2) \in \text{Image}(\mu)} \delta_{(\alpha_1, \alpha_2)}(H'_{(\alpha_1, \alpha_2)}),$$

where

$$H'_{(\alpha_1, \alpha_2)} := D_{(\alpha_1, \alpha_2)}(K) \cap \psi_{(\alpha_1, \alpha_2)}^{-1}(\mathbb{P}^1(\mathbb{Q})),$$

with $\psi_{(\alpha_1, \alpha_2)} : D_{(\alpha_1, \alpha_2)} \rightarrow \mathbb{P}^1$ and $\psi_{(\alpha_1, \alpha_2)}(x, y_1, y_2, y_3) = (x, 1)$.

A computation gives that

$$\text{Kernel}(\overline{N}) \cap (\mathbb{Q}(2, S_1) \times K(2, S_2)) = \{(1, 1), (1, -1), (23, 5 - \theta), (23, \theta - 5)\},$$

so we only need to be concerned with the covers $D_1 = D_{(1,1)}$, $D_2 = D_{(1,-1)}$, $D_3 = D_{(23,5-\theta)}$ and $D_4 = D_{(23,\theta-5)}$. Finally it is obvious that

$$\begin{aligned} H'_{(1,1)} &= \gamma_1^{-1}(H_1) \\ H'_{(1,-1)} &= \gamma_2^{-1}(H_2) \\ H'_{(23,5-\theta)} &= \gamma_3^{-1}(H_3) \\ H'_{(23,\theta-5)} &= \gamma_4^{-1}(H_4). \end{aligned}$$

□

We can now prove the following

Theorem 5.2. *The only \mathbb{Q} -rational point on the curve Y defined by the equation*

$$y^2 = (x^3 + x^2 - 1)\Phi_{11}(x)$$

is the point at infinity.

Proof. We have that

$$Y(\mathbb{Q}) = \bigcup_{i=1}^4 \delta_i (\gamma_i^{-1}(H_i)).$$

from Lemma 5.1 and that $H_1 = H'_1$, $H_2 = H'_2$ and $H_3 = H'_3$ from Lemma 4.3. Also a 2-Selmer group computation shows that $J_4(K) = \{0\}$, where J_4 is the Jacobian variety of C_4 and thus $H_4 = C_4(K) = \{(1, 0, 0)\}$. So putting these together we get that

$$\begin{aligned} Y(\mathbb{Q}) &= \delta_1 (\gamma_1^{-1} (\{(-1, -1, 1), (-1, 1, 1), (1, 0, 0)\})) \\ &\quad \cup \delta_2 (\gamma_2^{-1} (\{(0, 1, 1), (0, -1, 1), (1, 0, 0)\})) \\ &\quad \cup \delta_3 (\gamma_3^{-1} (\{(1, 0, 0)\})) \\ &\quad \cup \delta_4 (\gamma_4^{-1} (\{(1, 0, 0)\})) \\ &= \{\infty\} \cup \{\infty\} \cup \{\infty\} \cup \{\infty\} \\ &= \{\infty\}. \end{aligned}$$

□

REFERENCES

- [1] W. BOSMA, J. CANNON, AND C. PLAYOUST, *The Magma algebra system. I. The user language*, J. Symbolic Comput., 24 (1997), pp. 235–265. Computational algebra and number theory (London, 1993).
- [2] N. BRUIN, *Chabauty methods using elliptic curves*, J. Reine Angew. Math., 562 (2003), pp. 27–49.
- [3] N. BRUIN AND N. D. ELKIES, *Trinomials ax^7+bx+c and ax^8+bx+c with Galois groups of order 168 and $8 \cdot 168$* , in Algorithmic number theory (Sydney, 2002), vol. 2369 of Lecture Notes in Comput. Sci., Springer, Berlin, 2002, pp. 172–188.
- [4] N. BRUIN AND M. STOLL, *Deciding existence of rational points on curves: an experiment*, Experiment. Math., 17 (2008), pp. 181–189.
- [5] Y. BUGEAUD, M. MIGNOTTE, S. SIKSEK, M. STOLL, AND S. TENGELY, *Integral points on hyperelliptic curves*, Algebra Number Theory, 2 (2008), pp. 859–885.
- [6] C. CHABAUTY, *Sur les points rationnels des variétés algébriques dont l'irrégularité est supérieure à la dimension*, C. R. Acad. Sci. Paris, 212 (1941), pp. 1022–1024.
- [7] R. F. COLEMAN, *Effective Chabauty*, Duke Math. J., 52 (1985), pp. 765–770.
- [8] ———, *Torsion points on curves and p -adic abelian integrals*, Ann. of Math. (2), 121 (1985), pp. 111–168.
- [9] B. POONEN AND E. F. SCHAEFER, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math., 488 (1997), pp. 141–188.
- [10] S. SIKSEK, *Explicit chabauty over number fields*, (2011). arXiv:1010.2603v2.
- [11] M. STOLL, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith., 98 (2001), pp. 245–277.

MATHEMATICS INSTITUTE, UNIVERSITY OF WARWICK
E-mail address: M.Mourao@warwick.ac.uk